Front. Comput. Sci., 2025, 19(9): 199609
https://doi.org/10.1007/s11704-024-40474-y

REVIEW ARTICLE

Graph neural networks for financial fraud detection: a review

Dawei CHENG[1,2,3], **Yao ZOU**[1,3], **Sheng XIANG**[4], **Changjun JIANG** (✉)[1,2,3]

1 Department of Computer Science and Technology, Tongji University, Shanghai 200092, China
2 Shanghai Artificial Intelligence Laboratory, Shanghai 200031, China
3 National Collaborative Innovation Center for Internet Financial Security, Shanghai 100045, China
4 AAII, University of Technology Sydney, Sydney 2007, Australia

Abstract The landscape of financial transactions has grown increasingly complex due to the expansion of global economic integration and advancements in information technology. This complexity poses greater challenges in detecting and managing financial fraud. This review explores the role of Graph Neural Networks (GNNs) in addressing these challenges by proposing a unified framework that categorizes existing GNN methodologies applied to financial fraud detection. Specifically, by examining a series of detailed research questions, this review delves into the suitability of GNNs for financial fraud detection, their deployment in real-world scenarios, and the design considerations that enhance their effectiveness. This review reveals that GNNs are exceptionally adept at capturing complex relational patterns and dynamics within financial networks, significantly outperforming traditional fraud detection methods. Unlike previous surveys that often overlook the specific potentials of GNNs or address them only superficially, our review provides a comprehensive, structured analysis, distinctly focusing on the multifaceted applications and deployments of GNNs in financial fraud detection. This review not only highlights the potential of GNNs to improve fraud detection mechanisms but also identifies current gaps and outlines future research directions to enhance their deployment in financial systems. Through a structured review of over 100 studies, this review paper contributes to the understanding of GNN applications in financial fraud detection, offering insights into their adaptability and potential integration strategies.

Keywords financial fraud detection, graph neural networks, data mining

1 Introduction

The rapid development of global economic integration and information technology in recent years has led to a significant increase in the scale and complexity of financial sector transactions. However, this expansion also brings about a broader range of financial fraud risks, resulting in a rise in criminal activities [1,2]. According to a report by the Canadian Anti-Fraud Centre (CAFC), fraud losses in 2023 alone reached 554 million, marking a 4.3% increase compared to the previous year, indicating an ongoing upward trend [3]. This data indicates that financial fraud not only causes direct economic losses to victims and businesses but also erodes public trust in the entire financial system [4]. Therefore, it is crucial to build a financial fraud detection system to prevent unauthorized financial gain through illegal or deceptive means.

Traditional rule-based systems and classic machine learning methods have been used for fraud detection, but they often struggle with complex fraud patterns on large amounts of financial data [5–11]. In contrast, deep learning has shown exceptional performance in various domains, leveraging its ability to learn intricate features from raw data [12–15]. Recent survey papers have demonstrated that deep learning models outperform traditional methods in terms of accuracy, adaptability, and scalability [16–18]. Some fraud detection models, such as those leveraging Graph Neural Networks (GNNs), have achieved remarkable progress and exhibited superior performance in the financial domain [19–23]. Utilizing deep learning techniques on graph, GNNs can ascertain advanced feature representations of nodes and edges, thereby identifying complex fraud patterns that may remain obscured within traditional data representations [24]. For example, analyzing transaction networks enables the detection of complex fraudulent activities such as money laundering, credit card fraud, and insurance fraud [25–32].

Despite the potential of GNNs in fraud detection, there are practical challenges that need to be addressed. These include managing large-scale financial graph data and ensuring model adaptability to dynamic patterns [33–37]. Additionally, transparency and interpretability of models are critical for enhancing the confidence of financial institutions [38–40]. To delve deeper into the existing challenges for GNNs in financial fraud detection, this study proposes the following detailed research questions (RQs):

- **RQ1: How can various GNN methodologies in financial fraud detection be understood through a unified framework?**

Received May 11, 2024; accepted October 20, 2024

E-mail: cjjiang@tongji.edu.cn

- **RQ2: Why use GNNs for financial fraud detection? What roles do they play?**
- **RQ3: How to design GNNs suitable for financial fraud detection?**
- **RQ4: How are GNNs deployed in real-world financial fraud detection scenarios, and what are their impacts?**
- **RQ5: What are the current challenges and future directions for GNNs in financial fraud detection?**

To address these research questions, our contributions, summarized as follows, are designed to offer a holistic view of GNNs in financial fraud detection.

- **Establishing a unified framework:** We propose a comprehensive framework for categorizing and analyzing GNN methodologies in financial fraud detection, enhancing the clarity and depth of our understanding of this field. For a practical implementation of these methodologies, the AntiFraud project provides an open-source example on GitHub (See github.com/AI4Risk/antifraud website), which demonstrates the application of these techniques.
- **Exploring the suitability of GNNs:** We provide a detailed examination of why GNNs are uniquely positioned to address financial fraud detection, emphasizing their intrinsic capabilities.
- **Design considerations for GNNs:** We offer insights into the nuanced design process of GNNs tailored for financial fraud detection, focusing on how architectural and strategic choices impact their effectiveness.
- **Highlighting real-world applications:** We showcase examples of GNNs in action within the financial sector, discussing the outcomes and implications. Additional resources and examples can be found in the AntiFraud GitHub project (See github.com/AI4Risk/awesome-graph-based-fraud-detection website), which provides various implementations related to graph-based fraud detection.
- **Charting future directions:** We explore the landscape of current challenges and future opportunities in GNN research for financial fraud detection, aiming to inspire further innovation in this field.

Differences between this survey and existing ones. While there are numerous reviews that explore various machine learning techniques in financial fraud detection [19,41–47], these generally focus on conventional methods and often overlook the potential of GNN. For instance, studies [19,41,44,45,47] discuss a wide range of deep learning technologies applied in fraud detection but neglect GNNs, while [43] and [48] address GNN applications in specific subdomains, without covering the financial fraud detection field comprehensively. Moreover, although some surveys [4] briefly introduce systems based on graph learning, they merely touch upon the application of GNNs in financial fraud detection and do not delve deep. Another review [49], attempts to categorize GNN applications from multiple perspectives but focuses more on the technical framework rather than their practical utility in detecting financial fraud. These publications do not discuss in depth the advantages and limitations of GNN technologies.

This review not only summarizes the existing literature but also explores the advantages of GNN technologies, relevant architectural choices, current challenges, and future directions. By classifying and examining over 100 relevant studies, this paper aims to provide a detailed reference for further research and application of GNNs in the domain of financial fraud detection. This review paper points out that future research is anticipated to concentrate on augmenting the scalability, adaptability, and interpretability of GNNs, exploring cross-domain methodologies and multimodal data integration to bolster financial fraud detection and ensure financial security. Figure 1 represents the road map of the rest of the paper. We introduced the main GNN methods in Section 3. Then Sections 4 and 5 introduce the reason to choose GNNs and GNN design in the financial field for GNNs, respectively.

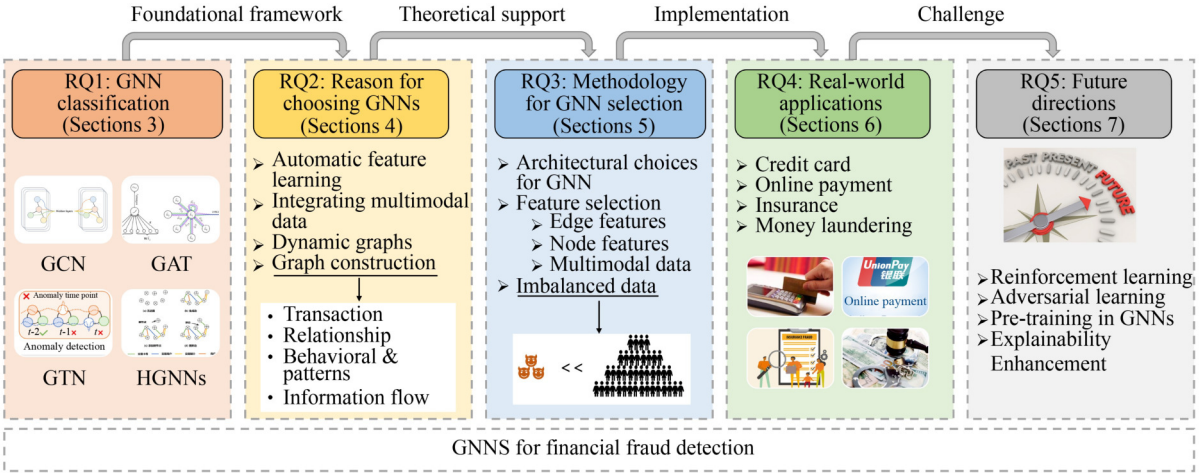

Fig. 1 An overview of the road map of this paper. We first introduce the mainly utilized graph neural networks (GNNs) for financial fraud detection. Secondly, we summarize the reasons for choosing GNNs. After that, we introduce the methods and special tricks in GNN architecture design for financial fraud detection tasks. Then we go through the real-world applications and future directions for GNN-based financial fraud detection

Table 1 The summary of notations in this paper

Symbol	Description
G	Graph
V	Set of nodes
E	Set of edges
n	Number of nodes
$\boldsymbol{I}_n \in \mathbb{R}^{n\times n}$	Identity matrix
$\boldsymbol{A} \in \mathbb{R}^{n\times n}$	Adjacency matrix
$\boldsymbol{D} \in \mathbb{R}^{n\times n}$	Degree matrix (diagonal)
$\boldsymbol{L} \in \mathbb{R}^{n\times n}$	Laplacian matrix
$\boldsymbol{U} \in \mathbb{R}^{n\times n}$	Eigenvector matrix
$\boldsymbol{\Lambda} \in \mathbb{R}^{n\times n}$	Eigenvalue matrix (diagonal)
$\boldsymbol{u}_i \in \mathbb{R}^n$	ith eigenvector
$\boldsymbol{X} \in \mathbb{R}^{n\times D}$	Node feature matrix
$\boldsymbol{x}_i \in \mathbb{R}^D$	Features of the ith node
$\boldsymbol{f} \in \mathbb{R}^n$	Signal

2 Preliminaries

2.1 Problem definitions

In this section, we first provide the definitions of the common notations used, as shown in Table 1. We define graph $G = (V, E, \boldsymbol{A})$ as an undirected graph, where V is the set of nodes, $|V| = n$ is the number of nodes, E is the set of edges, and $\boldsymbol{A} \in \mathbb{R}^{n\times n}$ is the adjacency matrix; the entry $\boldsymbol{A}_{i,j}$ of the matrix is 1 if there is an edge between nodes i and j, and 0 otherwise. The degree matrix $\boldsymbol{D} \in \mathbb{R}^{n\times n}$ is a diagonal matrix where each entry $\boldsymbol{D}_{i,i}$ is the sum of the ith row of $\boldsymbol{A}$, $\sum_j \boldsymbol{A}_{i,j}$. The graph Laplacian matrix is defined as $\boldsymbol{L} = \boldsymbol{I}_n - \boldsymbol{D}^{-\frac{1}{2}}\boldsymbol{A}\boldsymbol{D}^{-\frac{1}{2}}$, where $\boldsymbol{I}_n \in \mathbb{R}^{n\times n}$ is the identity matrix. The symmetric normalized Laplacian matrix is another form of the Laplacian matrix, defined as $\boldsymbol{L} = \boldsymbol{U}\boldsymbol{\Lambda}\boldsymbol{U}^\top$. Here $\boldsymbol{U} = \{\boldsymbol{u}_i | i = 1, \ldots, n\}$ is the matrix of eigenvectors, and $\boldsymbol{\Lambda} = \text{diag}(\{\lambda_i | i = 1, \ldots, n\})$ is the diagonal matrix of eigenvalues, and $\boldsymbol{u}_i$ is the ith eigenvector. We define $\boldsymbol{X} \in \mathbb{R}^{n\times D}$ as the node feature matrix of graph G, where $\boldsymbol{x}_i \in \mathbb{R}^D$ is the feature vector of node i. Then we introduce some extended definitions as follows:

Homogeneous and heterogeneous graphs. A graph $G = (V, E)$ can be extended to a heterogeneous graph defined as $G = (V, E, \phi, \psi)$, where $\phi : V \to \mathcal{A}$ assigns types to nodes and $\psi : E \to \mathcal{R}$ assigns types to edges. A graph is *homogeneous* if ϕ and ψ each map to a single type; otherwise, it is *heterogeneous*.

Multi-relation graph. A multi-relation graph is a graph where edges have different types.

Dynamic graph. A dynamic graph is defined as a sequence of graphs $G^{seq} = \{G_1, \ldots, G_T\}$, where $G_i = (V_i, E_i)$, for $i = 1, \ldots, T$, where V_i, E_i are the set of nodes and edges for the ith graph in the sequence respectively.

2.2 Graph neural networks

Typically, GNNs employ a message passing mechanism that incrementally aggregates information from the neighborhoods. Specifically, the message passing process at the kth layer in a GNN is delineated in two primary phases:

$$\boldsymbol{m}_i^{(k)} = \text{AGGREGATE}\left(\{\boldsymbol{h}_j^{(k-1)} : j \in \mathcal{N}(i)\}\right), \tag{1}$$

$$\boldsymbol{h}_i^{(k)} = \text{UPDATE}\left(\boldsymbol{h}_i^{(k-1)}, \boldsymbol{m}_i^{(k)}, \boldsymbol{x}_i\right), \tag{2}$$

where $\mathcal{N}(i)$ denotes the set of neighboring nodes of node i, AGGREGATE represents a permutation invariant aggregation function, and $\boldsymbol{x}_i$ is the feature vector of node i from the node feature matrix $\boldsymbol{X}$. Following K iterations of message passing, the resultant node embeddings $\boldsymbol{H}^{(K)}$ are then employed to execute the designated task. Figure 2 illustrates the tasks of GNNs at the node, edge, and graph levels, and Table 2 provides a comprehensive summary of the tasks associated with each of these levels. We briefly introduce the tasks of GNNs at three different levels as follows:

Node-level: GNNs are instrumental in node classification for financial networks, determining the label of each node based on its attributes and relationships. They effectively classify nodes for detecting credit card [28–30,50] and insurance fraud [31,51] by analyzing transaction patterns and claimant-provider relationships within financial networks.

Edge-level: At the edge level, GNNs are utilized for tasks such as edge classification and link prediction, which are pivotal for predicting fraudulent transactions in finance [52,53].

Graph-Level: At the graph level, GNNs address challenges in graph classification and attribute prediction and are applicable in finance for systemic risk assessment [54].

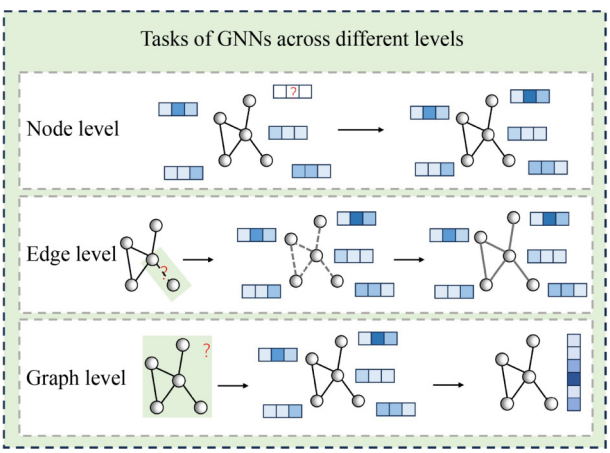

Fig. 2 The tasks of GNNs at different levels. For node level, the label of each node is determined by its features and neighbors. For edge level, the label of each edge is determined by the features of source & target node. For graph level, the property is determined by the features of all nodes or edges

Table 2 Summary of tasks across different levels in financial fraud detection

Level	Graph tasks	Application scenarios
Node	Node classification	Credit card fraud detection, insurance fraud detection, etc.
Edge	Edge classification, link prediction	Fraudulent transaction prediction, etc.
Graph	Graph classification, attribute prediction	Systemic risk assessment, etc.

3 Graph neural networks in financial fraud detection

This survey provides an in-depth exploration of GNNs applied in the domain of financial fraud detection, a critical area demanding advanced analytical techniques due to its complex and dynamic nature. Over the past five years, we have rigorously reviewed more than 100 high-quality papers from prestigious conferences and journals. This section categorizes the GNNs in financial fraud detection into four main types, reflecting the evolving landscape of graph-based deep learning technologies.

3.1 Graph convolutional networks

Graph convolutional networks (GCNs) process data structured in graph form, effectively identifying cross-transaction fraudulent activity patterns within transaction networks. The graph convolution operation on a graph $G=(V,E,\boldsymbol{A})$ is formalized as:

$$\boldsymbol{H}^{(k+1)}=\sigma(\hat{\boldsymbol{D}}^{-\frac{1}{2}}\hat{\boldsymbol{A}}\hat{\boldsymbol{D}}^{-\frac{1}{2}}\boldsymbol{H}^{(k)}\boldsymbol{W}^{(k)}), \tag{3}$$

where $\hat{\boldsymbol{A}}=\boldsymbol{A}+\boldsymbol{I}_n$ and $\hat{\boldsymbol{D}}$ is the degree matrix of $\hat{\boldsymbol{A}}$. The modified adjacency matrix $\hat{\boldsymbol{A}}$ ensures that each node has a self-loop, which is crucial for capturing the node's own information in its feature updates. The normalization step ensures that the influence of each neighbor is balanced, preventing any single node's impact from dominating the feature updates. This highlights GCNs' capability in uncovering subtle irregularities in financial transactions.

GCNs efficiently learn features and recognize patterns in financial data by capturing local connectivity and automatically discerning node and edge features. However, GCNs can suffer from over-smoothing, leading to the loss of distinct node characteristics, and are prone to overfitting with limited data.

3.2 Graph attention networks

Graph attention networks (GATs) employ an attention mechanism, allowing the model to focus on the most relevant parts of the graph. The attention coefficients can be computed as:

$$\alpha_{ij}=\frac{\exp(\text{LeakyReLU}(\boldsymbol{a}^{\top}[\boldsymbol{W}\boldsymbol{h}_i\|\boldsymbol{W}\boldsymbol{h}_j]))}{\sum_{k\in\mathcal{N}(i)}\exp(\text{LeakyReLU}(\boldsymbol{a}^{\top}[\boldsymbol{W}\boldsymbol{h}_i\|\boldsymbol{W}\boldsymbol{h}_k]))}, \tag{4}$$

where α_{ij} represents the importance of node j's features to node i, $\cdot^{\top}$ denotes transposition and $\|$ is the concatenation operation. The updated features for a node i are then computed as a weighted sum of the features of its neighbors:

$$\boldsymbol{h}_i'=\sigma\left(\sum_{j\in\mathcal{N}(i)}\alpha_{ij}\boldsymbol{W}\boldsymbol{h}_j\right). \tag{5}$$

To stabilize the learning process of self-attention, multi-head attention mechanism is applied, resulting in the following output feature representation:

$$\boldsymbol{h}_i'=\|_{k=1}^{K}\sigma\left(\sum_{j\in\mathcal{N}_{(i)}}\alpha_{ij}^{k}\boldsymbol{W}^{k}\boldsymbol{h}_j\right), \tag{6}$$

where α_{ij}^{k} are normalized attention coefficients computed by the kth attention mechanism, and $\boldsymbol{W}^{k}$ is the corresponding input linear transformation's weight matrix.

Specially, if we perform multi-head attention on the final layer of the network, it can be mathematically formulated as:

$$\boldsymbol{h}_i'=\sigma\left(\frac{1}{K}\sum_{k=1}^{K}\sum_{j\in\mathcal{N}_{(i)}}\alpha_{ij}^{k}\boldsymbol{W}^{k}\boldsymbol{h}_j\right). \tag{7}$$

The attention mechanism is particularly useful in applications such as financial fraud detection [55]. GATs outperform GCNs by dynamically allocating attention weights to neighbors, enabling adaptive focus on relevant nodes for improved complex pattern detection in financial fraud.

3.3 Graph temporal networks

Graph temporal networks (GTNs) incorporate the dynamic changes in financial transactions, utilizing expressions like:

$$\boldsymbol{H}^{(t+1)}=\sigma(\boldsymbol{A}^{(t)}\boldsymbol{H}^{(t)}\boldsymbol{W}^{(t)}), \tag{8}$$

to capture dynamic transactional data. These networks are particularly effective in identifying fraud within datasets sensitive to temporal patterns, such as credit card transactions and high-frequency trading [56,57]. To enhance the model's sensitivity to temporal dynamics, a temporal attention mechanism can be introduced, enabling the model to focus on the most significant parts of the graph at different times. For example, a temporal attention mechanism can be formulated as:

$$\alpha^{(t)}=\text{softmax}\left(\boldsymbol{q}^{\top}\tanh(\boldsymbol{W}_t\boldsymbol{H}^{(t)}+\boldsymbol{b}_t)\right), \tag{9}$$

$$\boldsymbol{H}_{\text{att}}^{(t)}=\sum_{t}\alpha^{(t)}\boldsymbol{H}^{(t)}, \tag{10}$$

where $\alpha^{(t)}$ are the attention weights at time t, determined by the learnable parameters $\boldsymbol{q}$, $\boldsymbol{W}_t$, and $\boldsymbol{b}_t$. The vector $\boldsymbol{q}$ is a query vector that projects the transformed node features into a scalar, thereby computing a preliminary attention score for each node. This score indicates the relevance or importance of each node's features at time t before normalization by the softmax function. Additionally, to accommodate multiple time steps and interactions between them, recurrent mechanisms can be employed:

$$\boldsymbol{H}^{(t)}=\text{GRU}(\boldsymbol{H}^{(t-1)},\boldsymbol{X}^{(t)}), \tag{11}$$

where $\boldsymbol{H}^{(t)}$ and $\boldsymbol{H}^{(t-1)}$ are the hidden states of the nodes at time t and $t-1$, respectively, $\boldsymbol{X}^{(t)}$ represents the input features at time t, and GRU denotes a gated recurrent unit used to integrate temporal information [58]. This addition of a recurrent layer allows the model to maintain a memory of past states, thus improving its ability to discern time-sensitive patterns that static GCNs cannot.

3.4 Heterogeneous graph neural networks

Heterogeneous graph neural networks (HGNNs) are designed to handle graphs composed of different types of nodes and edges, enabling the model to capture a richer set of relationships and properties within the data. To process heterogeneous graphs, it often employs a type-specific transformation mechanism, which can be mathematically

formulated as:

$$\boldsymbol{H}_a^{(k+1)} = \sigma\left(\sum_{r\in\mathcal{R}}\sum_{b\in\mathcal{A}} \boldsymbol{W}_{r,a,b}^{(k)} \cdot \mathrm{AGG}\left(\boldsymbol{H}_b^{(k)}, \boldsymbol{E}_{r,a,b}\right)\right), \tag{12}$$

where $\boldsymbol{H}_a^{(k)}$ represents the node features of type a at layer k, $\boldsymbol{W}_{r,a,b}^{(k)}$ is the weight matrix for relation r between node types a and b, $\boldsymbol{E}_{r,a,b}$ denotes the edges of type r between node types a and b, and AGG$(\cdot)$ is an aggregation function that combines features from neighboring nodes. The function σ is a non-linear activation. Common choices for AGG include sum, mean, and attention mechanisms, each providing different ways to emphasize the contributions of neighbors.

To enhance the capabilities of heterogeneous networks, the meta-path based approach [59–61] can be employed:

$$\boldsymbol{H}_{\text{meta}}^{(k+1)} = \sigma\left(\sum_{p\in\mathcal{P}} \boldsymbol{W}_p^{(k)} \cdot \mathrm{AGG}_p\left(\{\boldsymbol{H}_b^{(k)} \mid b \in \text{path}(p)\}\right)\right), \tag{13}$$

where $\boldsymbol{H}_{\text{meta}}^{(k+1)}$ indicates the updated node features along a specific meta-path p, $\boldsymbol{W}_p^{(k)}$ represents the weight matrix specific to meta-path p, and AGG_p is an aggregation function tailored to the meta-path p that considers node types and relations along the path. Meta-paths enable more complex relationships and structures to be utilized effectively, integrating context from multiple types of interactions.

Moreover, incorporating an attention mechanism [62–64] can dynamically weight the importance of different types of relationships:

$$\alpha_{r,a,b} = \mathrm{softmax}\left(\boldsymbol{q}_{r,a,b}^{\top}\sigma(\boldsymbol{W}_{r,a,b} \cdot \boldsymbol{H}_b^{(k)})\right), \tag{14}$$

$$\boldsymbol{H}_a^{(k+1)} = \sum_{r\in\mathcal{R}}\sum_{b\in\mathcal{A}} \alpha_{r,a,b} \cdot \boldsymbol{W}_{r,a,b}^{(k)} \cdot \boldsymbol{H}_b^{(k)}, \tag{15}$$

where $\alpha_{r,a,b}$ are attention weights that assess the relative importance of each neighboring node b of type b via relation r to node a, allowing the network to focus adaptively on the most informative parts of the heterogeneous structure.

3.5 GNN application overview

In exploring the down stream tasks of various GNNs for detecting financial fraud, Table 3 offers a comprehensive summarization. This table compiles a range of GNN approaches, including GCN, GAT, GTN, and HGNN, to illustrate their usage in financial fraud detection. Each method is collected based on its implementation details and characteristics, aiming to provide us with a clear perspective on which GNN strategies are effective in combating financial fraud.

GCNs such as Skip-GCN [65] and EWS-GCN [66] are adept at leveraging node and edge features but may fall short in capturing the temporal dynamics of fraud patterns. **GATs** like ASA-GNN [67] and ABGRL [68], offer adaptive attention mechanisms that enhance the detection of nuanced fraudulent behaviors, yet they can be computationally intensive. **GTNs** such as STAGN [20] and STGN [69], proficient in detecting time-sensitive fraud patterns, require more computational overhead due to their temporal attention modules. **HGNNs**, including LIFE [70] and MultiFraud [71], excel at integrating heterogeneous information, providing a rich context for fraud detection, but their complexity can be a double-edged sword, demanding more resources and making them less suitable for scalability-focused applications.

Despite their efficacy, GNNs encounter significant scalability challenges when scaling up to large financial networks. The high memory and computational demands on a single machine primarily stem from GPU memory constraints and the extensive time required for matrix multiplication operations. Additionally, in distributed environments, the high communication costs related to obtaining and combining graph embeddings of nodes' multi-hop neighbors in each training batch hinder the speed benefits of parallelization [12]. These challenges highlight the need for more efficient GNN architectures to handle larger financial networks with quick response times for real-time fraud detection.

4 Reasons to choose GNNs for financial fraud detection

GNNs have shown promising results in the field of financial fraud detection by leveraging their unique abilities to model complex relationships, learn features automatically, handle dynamic graphs, and integrate multimodal data. This section explores these aspects in detail, highlighting the versatility and effectiveness of GNNs in tackling the challenges associated with detecting fraudulent activities in financial systems.

Table 3 Summary of GNN methods for financial fraud detection

Approach	Category	Key idea	Level	Application
Skip-GCN (2019) [65]	GCN	Skip connection	Node level	Anti-money laundering
EWS-GCN (2020) [66]	GCN	Edge weight-shared convolution	Node level	Credit scoring
FMGAD (2023) [72]	GCN	Deep-GNN	Node level	Credit card fraud detection
Li et al. (2021) [73]	GAT	Self-attention mechanism	Node level	Credit card fraud detection
ASA-GNN (2023) [67]	GAT	Adaptive sampling and aggregation	Node level	Transaction fraud detection
ABGRL (2024) [68]	GAT	Adaptive attention convolution	Node level	Phishing accounts detection
STAGN (2020) [20]	GTN	Spatial-temporal attention module	Node level	Credit card fraud detection
STGN (2023) [69]	GTN	Spatial-temporal attention module	Node level	Credit card fraud detection
LIFE (2021) [70]	HGNN	Heterogeneous graph representation learning	Node level	Online payment fraud detection
C-FATH (2021) [64]	HGNN	Community-based filtering	Node level	Online payment fraud detection
CGNN (2022) [52]	HGNN	Competitive mechanism	Edge Level	E-commerce fraud detection
GoSage (2023) [63]	HGNN	Node level and relation level attention	Node level	Collusion fraud detection
MultiFraud (2024) [71]	HGNN	Multi-view representation learning	Node level	Supply chain fraud detection

4.1 Graph construction from financial data

To address the requirements of fraud detection within the financial sector, constructing financial-oriented graphs is essential for uncovering *abnormal transaction patterns*, *unusual behavioral interactions*, and *potential fraud clusters*. This subsection introduces various methods for constructing graphs based on financial data, aiming to facilitate the detection and prediction of fraudulent behavior.

Transaction graph construction. Transaction data is pivotal for revealing fraudulent activities. Creating a transaction network (graph), with nodes representing individual accounts or entities (such as individuals, companies) and edges representing transactions (e.g., transfers, payments) [74,75], enables the effective identification of abnormal transaction patterns [76]. For example, frequent small transactions or large funds flows within a short period may indicate fraudulent activity [77]. Analyzing the network's topology, such as node centrality and community divisions, can help identify fraud rings or key fraudulent accounts.

Relationship-based graph construction. Beyond direct transaction data, the relationships between financial entities are crucial for fraud detection [78]. Constructing complex network (graph) that include various entities (like individuals, companies, bank accounts) and their relationships (such as ownership, control relations) can reveal the cooperation networks behind complex fraudulent activities like money laundering or insider trading [79]. For example, Mao et al. utilize the inter-enterprise relationships to establish a network [80].

Behavioral and device pattern graph. Constructing graphs based on user behaviors and device usage patterns (e.g., logins, queries, transaction requests, device types, operating systems, and device IDs) can reveal the similarities or abnormal patterns between different accounts [81–83]. By connecting accounts whose behavior and device usage similarity exceeds a certain threshold, it's possible to uncover networks of accounts potentially operated by fraudsters. This includes identifying users who switch devices in patterns that deviate from typical user behavior, or who use devices known to be associated with fraudulent activities [58]. Such graphs significantly enhance machine learning models' ability to recognize atypical behavior and device usage patterns, thereby predicting and identifying potential fraud more effectively [24].

Information flow graph construction. Malicious actors often exploit misleading information for market manipulation. Constructing information flow graphs [84] by analyzing the relationship between public information (e.g., news, announcements, social media discussions) and financial market activities can help identify patterns of information manipulation and the centers of influence, thereby detecting related fraudulent activities [85–87].

These methods illustrate the diverse approaches to graph construction from financial data, each contributing uniquely to the identification and prediction of fraud.

4.2 Automatic feature learning

GNNs greatly enhance financial fraud detection through their ability to learn features automatically, unlike traditional machine learning methods that require extensive feature engineering. GNNs extract relevant features from graph data, which is crucial for keeping pace with the dynamic nature of financial fraud. The foundational layer of GNNs, the message passing mechanism, enables a sophisticated form of feature extraction. It integrates attributes from both nodes and edges, which are rich in data that can signal fraudulent activity. This mechanism effectively combines the influences of neighboring nodes and updates each node's features through successive layers. This iterative process allows GNNs to reveal complex and non-linear relationships within the data, typical of fraudulent activities [21]. The capacity for automatic feature learning —requiring no specific programming for feature identification —makes GNNs exceptionally effective at uncovering both sophisticated and previously undetected fraud schemes. Overall, the intrinsic feature learning of GNNs not only eases model development and training but also ensures rapid adaptation to new fraudulent tactics, playing a vital role in fighting financial crime.

4.3 Dynamic graphs

Financial networks are inherently dynamic, continuously evolving with the addition of new transactions, accounts, and users. This dynamic nature presents significant challenges for fraud detection systems, which must adapt to effectively detect emerging fraudulent schemes.

Challenges posed by dynamic financial graphs. The ever-changing structure of financial graphs complicates the task of fraud detection. As new nodes and edges are added, previously learned patterns may no longer apply, and new patterns of fraud can emerge. Traditional static models struggle to capture these evolving patterns, often leading to outdated or inaccurate fraud detection.

GNNs offer a promising solution to the challenge of modeling dynamic financial graphs. By incorporating the temporal aspect into their architecture, GNNs can update their node and edge representations in response to new information. Several approaches enhance GNNs' adaptability to dynamic graphs as follow:

Temporal attention mechanisms allow GNNs to weigh the importance of different transactions or behaviors over time, focusing on those most indicative of fraud. This is particularly effective in emphasizing recent transactions that may signal current fraudulent activities.

Time-decay functions [88] in the aggregation process enable GNNs to prioritize recent interactions, formalized as:

$$\boldsymbol{m}_i^{(k)}(t) = \text{AGGREGATE}\left(\{\alpha(t,t_j)\boldsymbol{h}_j^{(k-1)}(t_j) : j \in \mathcal{N}(i)\}\right), \quad (16)$$

$$\boldsymbol{h}_i^{(k)}(t) = \text{UPDATE}\left(\boldsymbol{h}_i^{(k-1)}(t), \boldsymbol{m}_i^{(k)}(t)\right), \quad (17)$$

where $\alpha(t,t_j)$ diminishes the influence of older interactions over time, emphasizing more recent data. Unlike GRUs, which

dynamically process temporal sequences, time-decay functions statically modulate past data's impact, ideal for prioritizing recent interactions.

Graph temporal networks [89] combine the spatial structure captured by GCNs with the temporal dynamics processed by RNNs, offering a robust framework for dynamic graph analysis. The specific details can be found in Section 3.3.

Dynamic embeddings. [90] update node representations over time to reflect the latest graph structure and interactions, facilitating the detection of new fraud patterns as they develop.

By leveraging dynamic graph modeling, GNNs can provide timely and accurate fraud detection, adapting to the evolving landscape of financial transactions.

4.4 Integrating multimodal data

Financial fraud detection often necessitates the analysis of multimodal data, which includes numerical transaction data, textual communication records, and categorical user attributes. The integration of such varied data types presents challenges, mainly due to their heterogeneity—numerical data, text, and categorical information each require distinct preprocessing techniques and feature extraction methods. However, this diversity also offers significant opportunities. By combining these different types of data, a more comprehensive and nuanced view of financial activities can be obtained, leading to more effective fraud detection strategies [43,91].

Multimodal data fusion. GNNs emerge as a powerful tool for fusing different types of data within a unified framework. GNNs can naturally accommodate multimodal data by representing them as nodes in a graph, where the edges capture the relationships between various data points [92]. For instance, a GNN can model transactions as nodes, with edges representing the flow of money between accounts, while incorporating textual data through node attributes or separate text-associated nodes linked to relevant transactions or accounts [93].

To effectively fuse multimodal data, a GNN can employ an approach such as:

$$z_i^{(l)} = \boldsymbol{W}^{(l)} \cdot \text{AGGREGATE}\left(\{\boldsymbol{h}_j^{(l)} : j \in \mathcal{N}(i)\}\right), \tag{18}$$

$$\boldsymbol{h}_i^{(l+1)} = \sigma\left(z_i^{(l)} + \boldsymbol{B}^{(l)} \cdot \boldsymbol{x}_i\right), \tag{19}$$

where $\boldsymbol{h}_i^{(l)}$ is the feature vector of node i at layer l, $\boldsymbol{W}^{(l)}$ and $\boldsymbol{B}^{(l)}$ are learnable parameters, σ is a non-linear activation function, AGGREGATE is a function that combines features from node i's neighbors, and $\boldsymbol{x}_i$ represents the multimodal data associated with node i, potentially combining numerical, textual, and categorical information into a unified representation. This modeling allows GNNs to leverage the rich, interconnected data landscape of financial transactions, providing a holistic view of financial activities. Through the integration of multimodal data, GNNs can uncover complex patterns of fraudulent behavior that might be overlooked when analyzing data sources in isolation. For more methods of integrating multimodal information, please refer to Section 5.2.3.

5 GNN design for financial fraud detection

In this section, we discuss the critical elements in designing GNNs tailored for effective financial fraud detection. Key considerations include the selection of appropriate GNN architectures, meticulous feature selection, and strategies for managing the challenge of imbalanced data to ensure robustness and effectiveness in detecting fraudulent activities.

5.1 Architectural choices for GNN

Selecting an optimal GNN architecture for financial fraud detection involves understanding the unique characteristics of financial data. Graph Convolutional Networks excel in structured data environments, capturing local transaction patterns effectively. Graph Attention Networks leverage attention mechanisms to emphasize important transactions or patterns, beneficial in scenarios with significant edge attributes. Graph Transformer Networks adeptly handle time-series data, tracking financial activities over periods. Heterogeneous Graph Neural Networks are designed for networks with diverse node and edge types, enabling comprehensive integration of various financial behaviors.

5.2 Feature selection

5.2.1 Node feature engineering

Node feature engineering in financial contexts is crucial. It involves a strategic analysis and extraction of node attributes, extending beyond basic transaction details like amount, frequency, and timing [94]. Advanced methodologies such as clustering for geographic transaction analysis [95], entropy measures for transaction diversity [96], and time-series analysis for cyclic patterns [97] significantly enrich the model' s dataset, enhancing its predictive power against fraud.

5.2.2 Edge features integration

Edge features are crucial in GNNs for enhancing fraud detection accuracy by representing dynamic relationships between nodes. Typically, these features are integrated as propagation weights to tailor information aggregation and highlight significant relationships, as explored by Wang et al., demonstrating its effectiveness in emphasizing critical transactional connections indicative of fraudulent activity [98]. Additionally, enhancing the message-passing mechanism by incorporating edge features with node data enriches interactions between nodes and captures complex relational patterns essential for detecting fraud, as shown by Gong et al. [99]. Preprocessing edge features before feeding them into the GNN, as highlighted by Zheng et al., creates enriched node or edge attributes, enhancing the initial data representation and overall learning efficacy, crucial for uncovering rare fraudulent patterns that might otherwise be missed by more straightforward models [100]. These techniques ensure that GNNs not only learn from but also emphasize the transactional connections most indicative of fraud, thereby enhancing the detection capabilities of financial fraud detection systems.

5.2.3 Multimodal data

Integrating multimodal data such as text, images, and

transaction logs is essential in enhancing GNNs for robust financial fraud detection. Multimodal data provides a richer representation of transactional contexts, enabling GNNs to detect complex fraudulent patterns effectively [92].

Self-attention weighted fusion. One effective technique is the use of self-attention weighted fusion, which dynamically adjusts the weights of different modal features to optimize data integration. Jia et al. developed a multi-modality self-attention aware deep network, originally designed for biomedical segmentation, demonstrating the effectiveness of this approach in handling complex, multimodal datasets [101].

Multimodal embedding fusion layers. Another approach is the use of multimodal embedding fusion layers that perform deep nonlinear transformations to merge data from various sources seamlessly. Kim and Chi's SAFFNet employs this technique for remote sensing scene classification, highlighting its potential to enhance feature integration across different modalities for improved classification accuracy [102].

Graph convolution interactions. Integrating graph structures with multimodal data through graph convolution interactions enhances models' analytical capabilities. Zhang et al. employed this to predict urban dynamics, illustrating its effectiveness in spatiotemporal forecasting [103]. Wei et al. developed MMGCN for personalized recommendations, showing its utility with diverse data types [104]. Lian et al. demonstrated its application in completing graphs for conversation systems, ensuring comprehensive data utilization [105].

These advancements highlight the importance of multimodal data integration in GNNs, significantly extending their applicability and effectiveness in financial fraud detection by providing a more comprehensive analysis of transactions across different modalities.

5.3 Imbalanced data

The prevalence of imbalanced data in financial fraud detection, where legitimate transactions vastly outnumber fraud cases, presents a significant challenge. Several strategies have been developed to address this issue, enhancing the model's performance in detecting minority class instances.

Graph data augmentation. Techniques such as node sampling or edge manipulation can effectively rebalance the dataset. Zhao et al. introduced GraphSMOTE, which innovatively applies the SMOTE technique for imbalanced node classification on graphs [106]. Similarly, Perez-Ortiz et al. discussed graph-based over-sampling methods tailored for ordinal regression, which can be adapted for fraud detection [107]. Wu et al. developed a GNN-based fraud detector that specifically tackles the challenges posed by graph disassortativity and imbalance in data [108].

Ensemble methods in graph learning. Aggregating predictions from various GNN models can improve accuracy on rare fraud cases. Pfeifer et al. explored the potential of federated ensemble learning with GNNs in the context of disease module discovery, which is analogous to fraud detection in its requirement for precise anomaly detection [109]. Shi et al. proposed a boosting algorithm for GNNs that effectively addresses imbalanced node classification [110].

Cost-sensitive GNN. Incorporating cost-sensitive learning approaches in GNNs involves adjusting the loss function to emphasize correct predictions on the minority class. Hu et al. designed a cost-sensitive GNN specifically for mobile social network fraud detection, increasing penalties for misclassifying fraud instances [111]. Duan et al. and Ma et al. also developed dual cost-sensitive and attention mechanisms, respectively, for imbalanced node classification [112,113].

Adaptive resampling in GNN. This strategy involves adjusting sampling rates based on current model performance to ensure balanced learning [114]. Zhang et al. detailed a hierarchical graph transformer with adaptive node sampling, optimizing sampling processes in real-time [115]. Hu et al. presented an adaptive two-layer light field compression scheme using a reconstruction method, which can be adapted for learning from imbalanced datasets [116].

Meta paths in heterogeneous graph networks. Utilizing meta paths in heterogeneous graphs enhances the detection capabilities for nuanced fraudulent activities by capturing complex semantic information [114]. Liang et al. discussed the use of meta-path-based heterogeneous graph neural networks in academic networks, which can be adapted for fraud detection [59]. Wang et al. developed a heterogeneous graph attention network that leverages meta paths to focus on important relationships within the graph [60]. Meng et al. explored discovering meta-paths in large heterogeneous information networks, highlighting their importance in enhancing model learning capabilities [61].

These strategies collectively ensure that GNNs are optimized to handle the complexities of financial data, providing robust solutions against financial fraud.

6 Application in financial fraud detection

GNNs have revolutionized the detection of fraudulent activities within diverse financial sectors. This section delves into the deployment of GNNs in key areas such as credit card fraud, online payment fraud, insurance fraud, and anti-money laundering efforts.

6.1 Credit card fraud detection

Credit card fraud detection represents a significant challenge within the financial industry, focusing on identifying unauthorized transactions to prevent financial losses. The adoption of GNNs has introduced innovative methods to address this issue by leveraging relational data among transactions, cardholders, and merchants. By modeling these elements as nodes and relationships as edges within a graph, GNNs capture both explicit and subtle fraudulent patterns effectively.

Significant contributions include the attribute-driven graph representation by Xiang et al. [28] within a semi-supervised learning framework, and the spatial-temporal attention mechanism by Cheng et al. [20], which significantly enhances

fraud detection accuracy. Nguyen et al. [117] emphasize the predictive power of future transaction data, while Van Belle et al. [118] introduce an inductive learning approach that improves generalization to new instances of fraud.

6.2 Online payment fraud detection

The detection of online payment fraud is critical for safeguarding digital financial transactions against various fraud types. GNNs, with their ability to model complex, dynamic relationships between transaction entities, have become a cornerstone in this domain. Notable developments include adaptive fraud detection frameworks in dynamic e-commerce environments by Zhang et al. [52], and dual-level learning architectures that utilize transactional layers to enhance detection accuracy by Zheng et al. [53]. Hierarchical attention mechanisms, as explored by Hu et al. [119], prioritize significant transactional features indicative of fraud. The application of heterogeneous graph models, such as those detailed by Liu et al. [62,120], effectively address multi-type relational data challenges, particularly in blockchain transactions.

6.3 Insurance fraud detection

In the insurance sector, GNNs analyze relational data among claims, providers, and patients to identify and predict fraudulent patterns. A notable application is Medicare fraud detection, where GNNs highlight inconsistencies in provider-patient interactions [121]. Techniques like risk diffusion in parallel GNN architectures address challenges associated with organized fraud groups, as noted by [31]. Dynamic GNNs, which adapt to evolving schemes of collaborative fraud, are also crucial for continuous learning in fraud detection [122,123]. These advancements demonstrate the effectiveness of GNNs in uncovering and mitigating insurance fraud.

6.4 Anti-money laundering detection

Anti-money laundering is a critical challenge in the financial sector, aimed at identifying and curbing illicit financial activities to obscure the origins of criminal proceeds. Graph neural networks have introduced transformative methods by modeling accounts, transactions, and entities as nodes and their relationships as edges in a graph. This approach enables GNNs to detect complex laundering patterns effectively.

Significant contributions to this field include the application of self-supervised graph representation learning strategies, as explored by Cardoso et al. [124], which enhance the model's ability to detect unusual patterns autonomously. Additionally, Cheng et al. [125] introduce group-aware deep graph learning approaches that improve the detection of coordinated laundering activities across multiple accounts. Furthermore, applications in cryptocurrency transactions have shown the potential of GNNs in financial forensics, with studies like those by Weber et al. [126] and Alarab et al. [127] experimenting with GNNs to tackle money laundering in Bitcoin transactions.

Overall, GNNs offer a transformative approach to detecting and predicting fraudulent activities, outperforming traditional detection methods by leveraging the connectivity inherent in financial transaction data.

7 Future directions

GNNs have shown remarkable potential for processing complex network data and enhancing fraud detection capabilities. As the field evolves, the following four research directions are pivotal for advancing the application of GNNs:

Integration of reinforcement learning with GNNs. As financial markets continue to evolve, there is a compelling need for models that can dynamically adjust and optimize in real-time. Reinforcement learning (RL) integrated with GNNs presents a promising approach to meet this demand. Initial studies, such as those by Munikoti et al. [128] and Kong et al. [129], have shown that RL can enhance the adaptability of GNNs, enabling them to effectively respond to changing transaction patterns and detect fraudulent activities more efficiently. Further investigations explore the diversity of approaches in enhancing GNNs with RL for fraud detection, demonstrating various strategies to optimize graph-based models for dynamic and accurate financial transaction analysis [58,130–133]. Future research should focus on developing models that further refine these adaptive capabilities, optimizing for real-time processing and decision-making across various financial scenarios. This could lead to more effective prediction and prevention of fraudulent activities by enabling continuous learning from transactional changes.

Application of adversarial learning in GNNs. The robustness of GNNs is critical in safeguarding against adversarial attacks, which simulate potential fraudulent activities. Adversarial learning enhances the accuracy and resilience of these models by training them to withstand various adversarial scenarios. Notable work in this area includes defending GNNs against adversarial attacks [134] and achieving certified robustness against structural perturbations [135]. Further studies such as those by Boyaci et al. [136] and Sun et al. [137] have extended this approach to different domains, including smart grids and general graph data systems. Future research should aim to develop more sophisticated adversarial training frameworks that expose GNNs to a broader array of attack scenarios, enhancing their efficacy and security in practical applications [138,139].

Pre-training in GNNs. Inspired by the successes of large pre-trained models in natural language processing, similar strategies could be adopted for GNNs to advance graph data processing in finance. This approach has shown potential in uncovering deeper patterns and improving fraud detection accuracy. For instance, Hu et al. [140] and Qiu et al. [141] have developed strategies and frameworks for pre-training GNNs on large and complex graph datasets. These techniques allow GNNs to learn useful representations before fine-tuning on specific tasks, enhancing performance across various domains. Further research should explore optimizing these models' training processes [142–144] and enhancing feature extraction from large datasets to effectively combat increasingly sophisticated fraud schemes [42,145].

Enhancing the explainability of GNNs. The explainability of decision-making models is critical for gaining trust from

regulators and users [146–148]. Future research should focus on developing methods or tools to elucidate GNNs' decision processes, aiming for greater transparency and understandability. Techniques could include advanced visualization methods to demonstrate how networks detect and react to fraudulent activities [149,150], or algorithms to clarify the significance of specific nodes and edges [151,152].

Enhancing the scalability of GNNs. Real-world financial networks, such as inter-bank transfer networks, often scale to millions of entities. This does not even account for the billions of historical unlabelled data points. Current single-machine single-GPU solutions can handle networks composed of up to ten million transactions [28]. Future research directions should consider leveraging multi-GPU setups to improve both training and inference efficiency. Additionally, utilizing disk space can increase the maximum size of transaction networks that can be processed. Furthermore, distributed computing frameworks should be considered to tackle billion scale fraud detection tasks using GNNs.

Exploring these directions will not only expand the application scope of GNNs in financial fraud detection but also provide a robust theoretical and practical foundation for the ongoing development of these technologies.

8 Conclusion

This study evaluates the efficacy of GNNs in the detection of financial fraud by addressing a set of comprehensive research questions that encompass the methodologies, roles, design, deployment, and challenges associated with GNNs within the financial fraud detection field. The introduction of a unified framework helps to systematize the diverse approaches observed in existing literature, offering a clearer understanding of how GNNs can be effectively applied in complex financial contexts. Our findings contribute to the body of knowledge by detailing the adaptive capabilities of GNNs to the dynamic nature of financial networks and emphasizing their potential to enhance fraud detection mechanisms. Moreover, this work identifies existing gaps and outlines prospective research directions that could further solidify the role of GNNs in improving fraud prevention systems. The insights provided here aim to guide future studies toward more nuanced applications and integration strategies for GNNs in real-world financial systems.

Acknowledgements This work was supported by the National Key R&D Program of China (No. 2022YFB4501704), the National Natural Science Foundation of China (Grant No. 62102287), and the Shanghai Science and Technology Innovation Action Plan Project (Nos. 22YS1400600 and 22511100700).

Competing interests The authors declare that they have no competing interests or financial conflicts to disclose.

References

1. AlFalahi L, Nobanee H. Conceptual building of sustainable economic growth and corporate bankruptcy. SSRN Electronic Journal, 2019
2. Máté D, Sadaf R, Oláh J, Popp J, Szűcs E. The effects of accountability, governance capital, and legal origin on reported frauds. Technological and Economic Development of Economy, 2019, 25(6): 1213−1231
3. CAFC. Financial fraud losses. See antifraudcentre-centreantifraude. ca/index-eng. htm, website, 2024
4. Motie S, Raahemi B. Financial fraud detection using graph neural networks: a systematic review. Expert Systems with Applications, 2024, 240: 122156
5. Alves R, Ferreira P M S, Belo O, Ribeiro J T S. Detecting telecommunications fraud based on signature clustering analysis. In: Proceedings of Business Intelligence Workshop of 13th Portugese Conference on Artificial Intelligence. 2007, 286−299
6. Seeja K R, Zareapoor M. FraudMiner: a novel credit card fraud detection model based on frequent itemset mining. The Scientific World Journal, 2014, 2014: 252797
7. Maes S, Tuyls K, Vanschoenwinkel B, Manderick B. Credit card fraud detection using Bayesian and neural networks. In: Proceedings of the 1st International NAISO Congress on NEURO FUZZY THECHNOLOGIES. 2002, 270
8. Ogwueleka F N. Data mining application in credit card fraud detection system. Journal of Engineering Science and Technology, 2011, 6(3): 311−322
9. Gaikwad J R, Deshmane A B, Somavanshi H V, Patil S V, Badgujar R A. Credit card fraud detection using decision tree induction algorithm. International Journal of Innovative Technology and Exploring Engineering, 2014, 4(6): 66−69
10. Ng A Y, Jordan M I. On discriminative vs. generative classifiers: a comparison of logistic regression and naive Bayes. In: Proceedings of the 14th International Conference on Neural Information Processing Systems: Natural and Synthetic. 2001, 841−848
11. Sahin Y, Duman E. Detecting credit card fraud by ANN and logistic regression. In: Proceedings of 2011 International Symposium on Innovations in Intelligent Systems and Applications. 2011, 315−319
12. Avrahami O, Lischinski D, Fried O. Blended diffusion for text-driven editing of natural images. In: Proceedings of 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022
13. Feng W, Zhu W, Fu J T, Jampani V, Akula A R, He X, Basu S, Wang X E, Wang W Y. LayoutGPT: compositional visual planning and generation with large language models. In: Proceedings of the 37th International Conference on Neural Information Processing Systems. 2023
14. Bai X, Wang X, Liu X, Liu Q, Song J, Sebe N, Kim B. Explainable deep learning for efficient and robust pattern recognition: a survey of recent developments. Pattern Recognition, 2021, 120: 108102
15. Lopez M M, Kalita J. Deep learning applied to NLP. 2017, arXiv preprint arXiv: 1703.03091
16. Popat R R, Chaudhary J. A survey on credit card fraud detection using machine learning. In: Proceedings of the 2nd International Conference on Trends in Electronics and Informatics. 2018, 1120−1125
17. Zheng W, Yan L, Gou C, Wang F Y. Federated meta-learning for fraudulent credit card detection. Proceedings of the Twenty-Ninth International Conference on International Joint Conferences on Artificial Intelligence. 2021, 4654−4660
18. Zhou X, Cheng S, Zhu M, Guo C, Zhou S, Xu P, Xue Z, Zhang W. A state of the art survey of data mining-based fraud detection and credit scoring. MATEC Web of Conferences, 2018, 189: 03002
19. Ahmed M, Mahmood A N, Islam M R. A survey of anomaly detection techniques in financial domain. Future Generation Computer Systems, 2016, 55: 278−288
20. Cheng D, Wang X, Zhang Y, Zhang L. Graph neural network for fraud detection via spatial-temporal attention. IEEE Transactions on Knowledge and Data Engineering, 2022, 34(8): 3800−3813

21. Hamilton W L, Ying R, Leskovec J. Inductive representation learning on large graphs. In: Proceedings of the 31st International Conference on Neural Information Processing Systems. 2017, 1025−1035
22. Li Y, Tam D S H, Xie S, Liu X, Ying Q F, Lau W C, Chiu D M, Chen S Z. Temporal graph representation learning for detecting anomalies in E-payment systems. In: Proceedings of 2021 International Conference on Data Mining Workshops. 2021, 983−990
23. Niepert M, Ahmed M, Kutzkov K. Learning convolutional neural networks for graphs. In: Proceedings of the 33rd International Conference on International Conference on Machine Learning. 2016, 2014−2023
24. Ma X, Wu J, Xue S, Yang J, Zhou C, Sheng Q Z, Xiong H, Akoglu L. A comprehensive survey on graph anomaly detection with deep learning. IEEE Transactions on Knowledge and Data Engineering, 2023, 35(12): 12012−12038
25. Alarab I, Prakoonwit S, Nacer M I. Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain. In: Proceedings of the 5th International Conference on Machine Learning Technologies. 2020, 23−27
26. Xia P, Ni Z, Xiao H, Zhu X, Peng P. A novel spatiotemporal prediction approach based on graph convolution neural networks and long short-term memory for money laundering fraud. Arabian Journal for Science and Engineering, 2022, 47(2): 1921−1937
27. Sheu G Y, Li C Y. On the potential of a graph attention network in money laundering detection. Journal of Money Laundering Control, 2022, 25(3): 594−608
28. Xiang S, Zhu M, Cheng D, Li E, Zhao R, Ouyang Y, Chen L, Zheng Y. Semi-supervised credit card fraud detection via attribute-driven graph representation. In: Proceedings of the 37th AAAI Conference on Artificial Intelligence. 2023, 14557−14565
29. Liu G, Tang J, Tian Y, Wang J. Graph neural network for credit card fraud detection. In: Proceedings of 2021 International Conference on Cyber-Physical Social Intelligence. 2021, 1−6
30. Syeda M, Zhang Y Q, Pan Y. Parallel granular neural networks for fast credit card fraud detection. In: Proceedings of 2002 IEEE World Congress on Computational Intelligence. 2002 IEEE International Conference on Fuzzy Systems. 2002, 572−577
31. Ma J, Li F, Zhang R, Xu Z, Cheng D, Ouyang Y, Zhao R, Zheng J, Zheng Y, Jiang C. Fighting against organized fraudsters using risk diffusion-based parallel graph neural network. In: Proceedings of the 32nd International Joint Conference on Artificial Intelligence. 2023, 6138−6146
32. Wu J, Liu X, Cheng D, Ouyang Y, Wu X, Zheng Y. Safeguarding fraud detection from attacks: a robust graph learning approach. In: Proceedings of the 33rd International Joint Conference on Artificial Intelligence. 2024, 7500−7508
33. Lin Z, Li C, Miao Y, Liu Y, Xu Y. PaGraph: scaling GNN training on large graphs via computation-aware caching. In: Proceedings of the 11th ACM Symposium on Cloud Computing. 2020, 401−415
34. Tan Z, Yuan X, He C, Sit M K, Li G, Liu X, Ai B, Zeng K, Pietzuch P, Mai L. Quiver: supporting GPUs for low-latency, high-throughput GNN serving with workload awareness. 2023, arXiv preprint arXiv: 2305.10863
35. Park Y, Min S, Lee J W. Ginex: SSD-enabled billion-scale graph neural network training on a single machine via provably optimal in-memory caching. Proceedings of the VLDB Endowment, 2022, 15(11): 2626−2639
36. Zhang Z, Wang X, Zhang Z, Li H, Qin Z, Zhu W. Dynamic graph neural networks under spatio-temporal distribution shift. In: Proceedings of the 36th International Conference on Neural Information Processing Systems. 2024, 440
37. Kazemi S M, Goel R, Jain K, Kobyzev I, Sethi A, Forsyth P, Poupart P. Representation learning for dynamic graphs: a survey. The Journal of Machine Learning Research, 2020, 21(1): 70
38. Ying Z, Bourgeois D, You J, Zitnik M, Leskovec J. GNNExplainer: generating explanations for graph neural networks. In: Proceedings of the 33rd International Conference on Neural Information Processing Systems. 2019, 829
39. Wu Y, Wang X, Zhang A, He X, Chua T S. Discovering invariant rationales for graph neural networks. In: Proceedings of the 10th International Conference on Learning Representations. 2022
40. Sui Y, Wang X, Wu J, Lin M, He X, Chua T S. Causal attention for interpretable and generalizable graph classification. In: Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. 2022, 1696−1705
41. Ashtiani M N, Raahemi B. Intelligent fraud detection in financial statements using machine learning and data mining: a systematic literature review. IEEE Access, 2022, 10: 72504−72525
42. West J, Bhattacharya M. Intelligent financial fraud detection: a comprehensive review. Computers & Security, 2016, 57: 47−66
43. Ngai E W T, Hu Y, Wong Y H, Chen Y, Sun X. The application of data mining techniques in financial fraud detection: a classification framework and an academic review of literature. Decision Support Systems, 2011, 50(3): 559−569
44. Al-Hashedi K G, Magalingam P. Financial fraud detection applying data mining techniques: a comprehensive review from 2009 to 2019. Computer Science Review, 2021, 40(C): 100402
45. Yue D, Wu X, Wang Y, Li Y, Chu C H. A review of data mining-based financial fraud detection research. In: Proceedings of 2007 International Conference on Wireless Communications, Networking and Mobile Computing. 2007, 5519−5522
46. Sharma A, Kumar Panigrahi P. A review of financial accounting fraud detection based on data mining techniques. International Journal of Computer Applications, 2012, 39(1): 37−47
47. Ali A, Abd Razak S, Othman S H, Eisa T A E, Al-Dhaqm A, Nasser M, Elhassan T, Elshafie H, Saif A. Financial fraud detection based on machine learning: a systematic literature review. Applied Sciences, 2022, 12(19): 9637
48. Kim J Y, Cho S B. A systematic analysis and guidelines of graph neural networks for practical applications. Expert Systems with Applications, 2021, 184: 115466
49. Zhou J, Cui G, Hu S, Zhang Z, Yang C, Liu Z, Wang L, Li C, Sun M. Graph neural networks: a review of methods and applications. AI Open, 2020, 1: 57−81
50. Zou Y, Cheng D. Effective high-order graph representation learning for credit card fraud detection. In: Proceedings of the 33rd International Joint Conference on Artificial Intelligence. 2024, 7581−7589
51. Zhang R, Cheng D, Yang J, Ouyang Y, Wu X, Zheng Y, Jiang C. Pre-trained online contrastive learning for insurance fraud detection. In: Proceedings of the 38th AAAI Conference on Artificial Intelligence. 2024, 22511−22519
52. Zhang G, Li Z, Huang J, Wu J, Zhou C, Yang J, Gao J. eFraudCom: an E-commerce fraud detection system via competitive graph neural networks. ACM Transactions on Information Systems, 2022, 40(3): 47
53. Zheng W, Xu B, Lu E, Li Y, Cao Q, Zong X, Shen H. MIDLG: mutual information based dual level GNN for transaction fraud complaint verification. In: Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. 2023, 5685−5694
54. Balmaseda V, Coronado M, de Cadenas-Santiago G. Predicting systemic risk in financial systems using Deep Graph Learning. Intelligent Systems with Applications, 2023, 19: 200240

55. Veličković P, Cucurull G, Casanova A, Romero A, Liò P, Bengio Y. Graph attention networks. In: Proceedings of the 6th International Conference on Learning Representations. 2018
56. Wang D, Zhang Z, Zhou J, Cui P, Fang J, Jia Q, Fang Y, Qi Y. Temporal-aware graph neural network for credit risk prediction. In: Proceedings of 2021 SIAM International Conference on Data Mining. 2021, 702−710
57. Huang H, Wang P, Zhang Z, Zhao Q. A spatio-temporal attention-based GCN for anti-money laundering transaction detection. In: Proceedings of the 19th International Conference on Advanced Data Mining and Applications. 2023, 634−648
58. Jiang N, Duan F, Chen H, Huang W, Liu X. MAFI: GNN-based multiple aggregators and feature interactions network for fraud detection over heterogeneous graph. IEEE Transactions on Big Data, 2022, 8(4): 905−919
59. Liang X, Ma Y, Cheng G, Fan C, Yang Y, Liu Z. Meta-path-based heterogeneous graph neural networks in academic network. International Journal of Machine Learning and Cybernetics, 2022, 13(6): 1553−1569
60. Wang X, Ji H, Shi C, Wang B, Ye Y, Cui P, Yu P S. Heterogeneous graph attention network. In: Proceedings of the World Wide Web Conference. 2019, 2022−2032
61. Meng C, Cheng R, Maniu S, Senellart P, Zhang W. Discovering meta-paths in large heterogeneous information networks. In: Proceedings of the 24th International Conference on World Wide Web. 2015, 754–764
62. Liu C, Sun L, Ao X, Feng J, He Q, Yang H. Intention-aware heterogeneous graph attention networks for fraud transactions detection. In: Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining. 2021, 3280−3288
63. Ghosh S, Anand R, Bhowmik T, Chandrashekhar S. GoSage: heterogeneous graph neural network using hierarchical attention for collusion fraud detection. In: Proceedings of the 4th ACM International Conference on AI in Finance. 2023, 185−192
64. Wang L, Li P, Xiong K, Zhao J, Lin R. Modeling heterogeneous graph network on fraud detection: a community-based framework with attention mechanism. In: Proceedings of the 30th ACM International Conference on Information & Knowledge Management. 2021, 1959−1968
65. Weber M, Domeniconi G, Chen J, Weidele D K I, Bellei C, Robinson T, Leiserson C E. Anti-money laundering in bitcoin: experimenting with graph convolutional networks for financial forensics. 2019, arXiv preprint arXiv: 1908.02591
66. Sukharev I, Shumovskaia V, Fedyanin K, Panov M, Berestnev D. EWS-GCN: Edge weight-shared graph convolutional network for transactional banking data. In: Proceedings of 2020 IEEE International Conference on Data Mining. 2020, 1268−1273
67. Tian Y, Liu G, Wang J, Zhou M. ASA-GNN: adaptive sampling and aggregation-based graph neural network for transaction fraud detection. IEEE Transactions on Computational Social Systems, 2024, 11(3): 3536−3549
68. Sun H, Liu Z, Wang S, Wang H. Adaptive attention-based graph representation learning to detect phishing accounts on the ethereum blockchain. IEEE Transactions on Network Science and Engineering, 2024, 11(3): 2963−2975
69. Xie Y, Liu G, Zhou M, Wei L, Zhu H, Zhou R, Cao L. A spatial-temporal gated network for credit card fraud detection by learning transactional representations. IEEE Transactions on Automation Science and Engineering, 2024, 21(4): 6978−6991
70. Li Z, Wang H, Zhang P, Hui P, Huang J, Liao J, Zhang J, Bu J. Live-streaming fraud detection: a heterogeneous graph neural network approach. In: Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining. 2021, 3670−3678
71. Wu B, Chao K M, Li Y. Heterogeneous graph neural networks for fraud detection and explanation in supply chain finance. Information Systems, 2024, 121: 102335
72. Xu F, Wang N, Wen X, Gao M, Guo C, Zhao X. Few-shot message-enhanced contrastive learning for graph anomaly detection. In: Proceedings of the 29th IEEE International Conference on Parallel and Distributed Systems. 2023, 288−295
73. Li M, Sun M, Liu Q, Zhang Y. Fraud detection based on graph neural networks with self-attention. In: Proceedings of the 2nd International Seminar on Artificial Intelligence, Networking and Information Technology. 2021, 349−353
74. Altman E, Blanuša J, von Niederhäusern L, Egressy B, Anghel A, Atasu K. Realistic synthetic financial transactions for anti-money laundering models. In: Proceedings of the 37th International Conference on Neural Information Processing Systems. 2024, 1300
75. Singh K, Best P. Anti-money laundering: using data visualization to identify suspicious activity. International Journal of Accounting Information Systems, 2019, 34: 100418
76. Kim H, Choi J, Whang J J. Dynamic relation-attentive graph neural networks for fraud detection. In: Proceedings of 2023 IEEE International Conference on Data Mining Workshops. 2023, 1092−1096
77. Reurink A. Financial fraud: a literature review. Journal of Economic Surveys, 2018, 32(5): 1292−1325
78. Shi F, Zhao C. Enhancing financial fraud detection with hierarchical graph attention networks: a study on integrating local and extensive structural information. Finance Research Letters, 2023, 58: 104458
79. D'Arcangelis A M, Rotundo G. Complex networks in finance. In: Commendatore P, Matilla-García M, Varela L M, Cánovas J S, eds. Complex Networks and Dynamics: Social and Economic Interactions. Cham: Springer, 2016, 209−235
80. Mao X, Liu M, Wang Y. Using GNN to detect financial fraud based on the related party transactions network. Procedia Computer Science, 2022, 214: 351−358
81. Akoglu L, Tong H, Koutra D. Graph based anomaly detection and description: a survey. Data Mining and Knowledge Discovery, 2015, 29(3): 626−688
82. Egele M, Stringhini G, Krügel C, Vigna G. COMPA: detecting compromised accounts on social networks. In: Proceedings of the 20th Annual Network and Distributed System Security Symposium. 2013
83. Zou Y, Xiang S, Miao Q, Cheng D, Jiang C. Subgraph patterns enhanced graph neural network for fraud detection. In: Proceedings of the 29th International Conference on Database Systems for Advanced Applications. 2024, 375−384
84. Giudici P, Spelta A. Graphical network models for international financial flows. Journal of Business & Economic Statistics, 2016, 34(1): 128−138
85. Lu M, Han Z, Rao S X, Zhang Z, Zhao Y, Shan Y, Raghunathan R, Zhang C, Jiang J. BRIGHT - graph neural networks in real-time fraud detection. In: Proceedings of the 31st ACM International Conference on Information & Knowledge Management. 2022, 3342−3351
86. Innan N, Sawaika A, Dhor A, Dutta S, Thota S, Gokal H, Patel N, Khan M A Z, Theodonis I, Bennai M. Financial fraud detection using quantum graph neural networks. Quantum Machine Intelligence, 2024, 6(1): 7
87. Kurshan E, Shen H. Graph computing for financial crime and fraud detection: trends, challenges and outlook. International Journal of Semantic Computing, 2020, 14(4): 565−589
88. Kumar S, Zhang X, Leskovec J. Predicting dynamic embedding trajectory in temporal interaction networks. In: Proceedings of the 25th

ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. 2019, 1269−1278

89. Zhao L, Song Y, Zhang C, Liu Y, Wang P, Lin T, Deng M, Li H. T-GCN: a temporal graph convolutional network for traffic prediction. IEEE Transactions on Intelligent Transportation Systems, 2020, 21(9): 3848−3858
90. Du L, Wang Y, Song G, Lu Z, Wang J. Dynamic network embedding: an extended approach for skip-gram based network embedding. In: Proceedings of the 27th International Joint Conference on Artificial Intelligence. 2018, 2086−2092
91. Lahat D, Adali T, Jutten C. Multimodal data fusion: an overview of methods, challenges, and prospects. Proceedings of the IEEE, 2015, 103(9): 1449−1477
92. Cheng D, Yang F, Xiang S, Liu J. Financial time series forecasting with multi-modality graph neural network. Pattern Recognition, 2022, 121: 108218
93. Wu Z, Pan S, Chen F, Long G, Zhang C, Yu P S. A comprehensive survey on graph neural networks. IEEE Transactions on Neural Networks and Learning Systems, 2021, 32(1): 4−24
94. Ikeda C, Ouazzane K, Yu Q, Hubenova S. New feature engineering framework for deep learning in financial fraud detection. International Journal of Advanced Computer Science and Applications, 2021, 12(12): 10−21
95. Carpio-Pinedo J, Romanillos G, Aparicio D, Martín-Caro M S H, García-Palomares J C, Gutiérrez J. Towards a new urban geography of expenditure: using bank card transactions data to analyze multi-sector spatiotemporal distributions. Cities, 2022, 131: 103894
96. Isik F. An entropy-based approach for measuring complexity in supply chains. International Journal of Production Research, 2010, 48(12): 3681−3696
97. Devaki R, Kathiresan V, Gunasekaran S. Credit card fraud detection using time series analysis. International Journal of Computer Applications, 2014, 3: 8−10
98. Wang B, Jiang B, Tang J, Luo B. Generalizing aggregation functions in GNNs: building high capacity and robust GNNs via nonlinear aggregation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2023, 45(11): 13454−13466
99. Gong L, Cheng Q. Exploiting edge features for graph neural networks. In: Proceedings of 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2019, 9211−9219
100. Zheng P, Guo X, Chen E, Qi L, Guan L. Edge-labeling based modified gated graph network for few-shot learning. Pattern Recognition, 2024, 150: 110264
101. Jia X, Liu Y, Yang Z, Yang D. Multi-modality self-attention aware deep network for 3D biomedical segmentation. BMC Medical Informatics and Decision Making, 2020, 20: 119
102. Kim J, Chi M. SAFFNet: self-attention-based feature fusion network for remote sensing few-shot scene classification. Remote Sensing, 2021, 13(13): 2532
103. Zhang L, Geng X, Qin Z, Wang H, Wang X, Zhang Y, Liang J, Wu G, Song X, Wang Y. Multi-modal graph interaction for multi-graph convolution network in urban spatiotemporal forecasting. Sustainability, 2022, 14(19): 12397
104. Wei Y, Wang X, Nie L, He X, Hong R, Chua T S. MMGCN: multi-modal graph convolution network for personalized recommendation of micro-video. In: Proceedings of the 27th ACM International Conference on Multimedia. 2019, 1437−1445
105. Lian Z, Chen L, Sun L, Liu B, Tao J. GCNet: graph completion network for incomplete multimodal learning in conversation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2023, 45(7): 8419−8432
106. Zhao T, Zhang X, Wang S. GraphSMOTE: imbalanced node classification on graphs with graph neural networks. In: Proceedings of the 14th ACM International Conference on Web Search and Data Mining. 2021, 833−841
107. Pérez-Ortiz M, Gutiérrez P A, Hervás-Martínez C, Yao X. Graph-based approaches for over-sampling in the context of ordinal regression. IEEE Transactions on Knowledge and Data Engineering, 2015, 27(5): 1233−1245
108. Wu J, Hu R, Li D, Ren L, Hu W, Zang Y. A GNN-based fraud detector with dual resistance to graph disassortativity and imbalance. Information Sciences, 2024, 669: 120580
109. Pfeifer B, Chereda H, Martin R, Saranti A, Clemens S, Hauschild A C, Beißbarth T, Holzinger A, Heider D. Ensemble-GNN: federated ensemble learning with graph neural networks for disease module discovery and classification. Bioinformatics, 2023, 39(11): btad703
110. Shi S, Qiao K, Yang S, Wang L, Chen J, Yan B. Boosting-GNN: boosting algorithm for graph networks on imbalanced node classification. Frontiers in Neurorobotics, 2021, 15: 775688
111. Hu X, Chen H, Chen H, Liu S, Li X, Zhang S, Wang Y, Xue X. Cost-sensitive GNN-based imbalanced learning for mobile social network fraud detection. IEEE Transactions on Computational Social Systems, 2024, 11(2): 2675−2690
112. Duan Y, Liu X, Jatowt A, Yu H T, Lynden S, Kim K S, Matono A. Dual cost-sensitive graph convolutional network. In: Proceedings of 2022 International Joint Conference on Neural Networks. 2022, 1−8
113. Ma C, An J, Bai X E, Bao H Q. Attention and cost-sensitive graph neural network for imbalanced node classification. In: Proceedings of 2022 IEEE International Conference on Networking, Sensing and Control. 2022, 1−6
114. Li E, Ouyang J, Xiang S, Qin L, Chen L. Relation-aware heterogeneous graph neural network for fraud detection. In: Proceedings of the 8th International Joint Conference on Web and Big Data. 2024, 240−255
115. Zhang Z, Liu Q, Hu Q, Lee C K. Hierarchical graph transformer with adaptive node sampling. In: Proceedings of the 36th International Conference on Neural Information Processing Systems. 2022, 21171−21183
116. Hu X, Shan J, Liu Y, Zhang L, Shirmohammadi S. An adaptive two-layer light field compression scheme using GNN-based reconstruction. ACM Transactions on Multimedia Computing, Communications, and Applications, 2020, 16(2s): 72
117. Nguyen V B, Dastidar K G, Granitzer M, Siblini W. The importance of future information in credit card fraud detection. In: Proceedings of the 25th International Conference on Artificial Intelligence and Statistics. 2022, 10067−10077
118. Van Belle R, Van Damme C, Tytgat H, De Weerdt J. Inductive graph representation learning for fraud detection. Expert Systems with Applications, 2022, 193: 116463
119. Hu B, Zhang Z, Shi C, Zhou J, Li X, Qi Y. Cash-out user detection based on attributed heterogeneous information network with a hierarchical attention mechanism. In: Proceedings of the 33rd AAAI Conference on Artificial Intelligence. 2019, 946−953
120. Liu Z, Chen C, Yang X, Zhou J, Li X, Song L. Heterogeneous graph neural networks for malicious account detection. In: Proceedings of the 27th ACM International Conference on Information and Knowledge Management. 2018, 2077−2085
121. Yoo Y, Shin D, Han D, Kyeong S, Shin J. Medicare fraud detection using graph neural networks. In: Proceedings of 2022 International Conference on Electrical, Computer and Energy Technologies. 2022, 1−5
122. Ren L, Hu R, Li D, Liu Y, Wu J, Zang Y, Hu W. Dynamic graph

neural network-based fraud detectors against collaborative fraudsters. Knowledge-Based Systems, 2023, 278: 110888

123. Zhang J, Yang F, Lin K, Lai Y. Hierarchical multi-modal fusion on dynamic heterogeneous graph for health insurance fraud detection. In: Proceedings of IEEE International Conference on Multimedia and Expo. 2022, 1-6
124. Cardoso M, Saleiro P, Bizarro P. LaundroGraph: self-supervised graph representation learning for anti-money laundering. In: Proceedings of the 3rd ACM International Conference on AI in Finance. 2022, 130−138
125. Cheng D, Ye Y, Xiang S, Ma Z, Zhang Y, Jiang C. Anti-money laundering by group-aware deep graph learning. IEEE Transactions on Knowledge and Data Engineering, 2023, 35(12): 12444−12457
126. Weber M, Domeniconi G, Chen J, Weidele D K I, Bellei C, Robinson T, Leiserson C E. Anti-money laundering in bitcoin: experimenting with graph convolutional networks for financial forensics. In: Proceedings of the 2nd KDD Workshop on Anomaly Detection in Finance. 2019
127. Li Z, He E. Graph neural network-based bitcoin transaction tracking model. IEEE Access, 2023, 11: 62109−62120
128. Munikoti S, Agarwal D, Das L, Halappanavar M, Natarajan B. Challenges and opportunities in deep reinforcement learning with graph neural networks: a comprehensive review of algorithms and applications. IEEE Transactions on Neural Networks and Learning Systems, 2023.
129. Kong L, Feng J, Liu H, Tao D, Chen Y, Zhang M. MAG-GNN: reinforcement learning boosted graph neural network. In: Proceedings of the 37th International Conference on Neural Information Processing Systems. 2024, 525
130. Dou Y, Liu Z, Sun L, Deng Y, Peng H, Yu P S. Enhancing graph neural network-based fraud detectors against camouflaged fraudsters. In: Proceedings of the 29th ACM International Conference on Information & Knowledge Management. 2020, 315−324
131. Chen J, Chen Q, Jiang F, Guo X, Sha K, Wang Y. SCN_GNN: a GNN-based fraud detection algorithm combining strong node and graph topology information. Expert Systems with Applications, 2024, 237: 121643
132. Huang M, Liu Y, Ao X, Li K, Chi J, Feng J, Yang H, He Q. AUC-oriented graph neural network for fraud detection. In: Proceedings of the ACM Web Conference 2022. 2022, 1311−1321
133. Li R, Liu Z, Ma Y, Yang D, Sun S. Internet financial fraud detection based on graph learning. IEEE Transactions on Computational Social Systems, 2023, 10(3): 1394−1401
134. Zhang X, Zitnik M. GNNGUARD: defending graph neural networks against adversarial attacks. In: Proceedings of the 34th International Conference on Neural Information Processing Systems. 2020, 777
135. Wang B, Jia J, Cao X, Gong N Z. Certified robustness of graph neural networks against adversarial structural perturbation. In: Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining. 2021, 1645−1653
136. Boyaci O, Umunnakwe A, Sahu A, Narimani M R, Ismail M, Davis K R, Serpedin E. Graph neural networks based detection of stealth false data injection attacks in smart grids. IEEE Systems Journal, 2022, 16(2): 2946−2957
137. Sun L, Dou Y, Yang C, Zhang K, Wang J, Yu P S, He L, Li B. Adversarial attack and defense on graph data: a survey. IEEE Transactions on Knowledge and Data Engineering, 2023, 35(8): 7693−7711
138. Singh A, Gupta A, Wadhwa H, Asthana S, Arora A. Temporal debiasing using adversarial loss based GNN architecture for crypto fraud detection. In: Proceedings of the 20th IEEE International Conference on Machine Learning and Applications. 2021, 391−396
139. Deng Z, Xin G, Liu Y, Wang W, Wang B. Contrastive graph neural network-based camouflaged fraud detector. Information Sciences, 2022, 618: 39−52
140. Hu W, Liu B, Gomes J, Zitnik M, Liang P, Pande V S, Leskovec J. Strategies for pre-training graph neural networks. In: Proceedings of the 8th International Conference on Learning Representations. 2020
141. Qiu J, Chen Q, Dong Y, Zhang J, Yang H, Ding M, Wang K, Tang J. GCC: graph contrastive coding for graph neural network pre-training. In: Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. 2020, 1150−1160
142. Wan X, Xu K, Liao X, Jin Y, Chen K, Jin X. Scalable and efficient full-graph gnn training for large graphs. Proceedings of the ACM on Management of Data, 2023, 1(2): 1−23
143. Yu H, Wang L, Wang B, Liu M, Yang T, Ji S. GraphFM: improving large-scale GNN training via feature momentum. In: Proceedings of the 39th International Conference on Machine Learning. 2022, 25684−25701
144. Bai Y, Li C, Lin Z, Wu Y, Miao Y, Liu Y, Xu Y. Efficient data loader for fast sampling-based GNN training on large graphs. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(10): 2541−2556
145. Najafabadi M M, Villanustre F, Khoshgoftaar T M, Seliya N, Wald R, Muharemagic E. Deep learning applications and challenges in big data analytics. Journal of Big Data, 2015, 2: 1
146. Rao Y, Mi X, Duan C, Ren X, Cheng J, Chen Y, You H, Gao Q, Zeng Z, Wei X. Know-GNN: an explainable knowledge-guided graph neural network for fraud detection. In: Proceedings of the 28th International Conference on Neural Information Processing. 2021, 159−167
147. Qin Z, Liu Y, He Q, Ao X. Explainable graph-based fraud detection via neural meta-graph search. In: Proceedings of the 31st ACM International Conference on Information & Knowledge Management. 2022, 4414−4418
148. Dai E, Wang S. Towards self-explainable graph neural network. In: Proceedings of the 30th ACM International Conference on Information & Knowledge Management. 2021, 302−311
149. Pandit S, Chau D H, Wang S, Faloutsos C. Netprobe: a fast and scalable system for fraud detection in online auction networks. In: Proceedings of the 16th international conference on World Wide Web. 2007, 201−210
150. Huang M L, Liang J, Nguyen Q V. A visualization approach for frauds detection in financial market. In: Proceedings of the 13th International Conference Information Visualisation. 2009, 197−202
151. Foster J G, Foster D V, Grassberger P, Paczuski M. Edge direction and the structure of networks. Proceedings of the National Academy of Sciences of the United States of America, 2010, 107(24): 10815−10820
152. Meng L, Xu G, Yang P, Tu D. A novel potential edge weight method for identifying influential nodes in complex networks based on neighborhood and position. Journal of Computational Science, 2022, 60: 101591

Dawei Cheng is an associate professor with the Department of Computer Science and Technology, Tongji University, China. Before that, he was a postdoctoral associate at MoE Key Laboratory of Artificial Intelligence, Department of Computer Science, Shanghai Jiao Tong University, China. He received the PhD degree in computer science from Shanghai Jiao Tong University, China. His research fields include graph learning, big data computing, data mining, and machine learning.

Yao Zou is a master's student majoring in computer science at Tongji University, China. Her research interests include graph machine learning in the financial field, graph fraud detection algorithms, and data mining.

Sheng Xiang is a PhD candidate in the Australian Artificial Intelligence Institute, School of Computer Science, University of Technology Sydney (UTS), Australia. He received his BSc degree from Shanghai Jiao Tong University, China. His research interests include graph machine learning in finance, graph generative algorithms, bipartite graph processing, and dynamic graph analytics.

Changjun Jiang received the PhD degree from the Institute of Automation, Chinese Academy of Sciences, China in 1995. He is currently the leader of the Key Laboratory of Embedded System and Service Computing (Ministry of Education), Tongji University, China. He is an academician of Chinese Academy of Engineering, China and an IET Fellow and an Honorary Professor with Brunel University London, UK. He has been the recipient of one international prize and seven prizes in the field of science and technology.